PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G09C 1/00 | A2

(11) International Publication Number: **WO 99/13448**

(43) International Publication Date: 18 March 1999 (18.03.99)

(21) International Application Number: PCT/US98/19239

(22) International Filing Date: 11 September 1998 (11.09.98)

(30) Priority Data:
08/928,360 12 September 1997 (12.09.97) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, MS PAL1–521, Palo Alto, CA 94303 (US).

(72) Inventor: KALAJAN, Kevin, E.; 2900 Broadway #F, Redwood City, CA 94062 (US).

(74) Agent: SOBON, Wayne, P.; Fish & Richardson P.C., Suite 100, 2200 Sand Hill Road, Menlo Park, CA 94025 (US).

(81) Designated States: CA, IL, JP, MX, NO, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: REMOTE ACCESS–CONTROLLED COMMUNICATION

(57) Abstract

A method for establishing an access–controlled communications path across a network between a client and a network resource, the client having a client network address, includes validating the client to produce a validated client network address, and allowing the client access to the network resource based upon the validated client network address.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

REMOTE ACCESS-CONTROLLED COMMUNICATION

BACKGROUND

The present invention relates generally to electronic communications.

Generally, when a client establishes an electronic communication path over a network with a server at a remote location the path may not be secure. That is, messages sent between client and server may be susceptible to interception or tampering. This is especially true in communications paths initiated over large networks such as the Internet. In such unsecured environments, transfer of confidential information can be risky.

As accessibility to the Internet from remote locations continues to become more widely available and convenient, utilizing the Internet to perform tasks such as remotely accessing electronic mail and databases becomes increasingly desirable. Some methods have been developed to allow a remote user to establish secure communications sessions. For example, a variety of encryption methods have been developed at several network levels, such as at the transport protocol level (with, e.g., HTTPS) and the application level (with, e.g., encryption of transported files). As another example, firewalls can prevent access to sensitive data from unauthorized Internet clients. Current one-time password schemes can be used to allow access to the resources of a web server or network. However, such schemes often allow public access to the authentication system, thus potentially leaving the system open to "hackers" or other potential intruders.

SUMMARY

In general, in one aspect, the invention features establishing an access-controlled communications path across a network between a client and a network resource, where the client has a client network address. The client is validated to produce a validated client network address, and the client is allowed access to the network resource based upon the validated client network address.

Embodiments of the invention may include one or more of the following features. A communications path can be established between the client and a destination network address coupled to the network resource. Access to the network resource can be allowed by configuring the network resource to selectively communicate with the validated client network address. Access to the network resource can be allowed by configuring the network resource to selectively accept packets from the validated client network address. The network resource can stop accepting packets from the client network address after the client terminates the access-controlled communications path, and can continue rejecting packets until the client network address is again validated. The network resource can block communication with at least one unvalidated network address. The network resource can drop packets from unvalidated network addresses. Access to the network resource can be allowed by opening a firewall to packets from the validated client network address. Establishing a communications path between the client and the destination network address can include establishing a communications path between the client and a server through the destination network address. The server can be an HTTP server. The client network address can be an Internet Protocol (IP) address. The access-controlled communications path can be terminated after a first predetermined time period, wherein information

relating to the time period can be indicated to the client. The information can include the time remaining in the time period, and how to extend the time period. The access-controlled communications path can be maintained for a first predetermined time period, after which the client can be revalidated and the access-controlled communications path maintained for a second predetermined time period based upon the revalidation. Validating can include requesting a first predetermined validation sequence from the client, and validating the client based upon a response. A second predetermined validation sequence can be requested in order to maintain the access-controlled communications path once it has been established. A derivative client can be validated in addition to the client, where the derivative client shares the client network address with the client, where the client establishes a first predetermined time period for the access-controlled communications path and the derivative client establishes a second predetermined time period for the access-controlled communications path. The first predetermined time period can be compared with the second predetermined time period to determine a longer time period, and the access-controlled communications path can be maintained based on the longer time period.

In general, in another aspect, the invention features apparatus for establishing an access-controlled communications path across a network between a client coupled to the network and a server coupled to the network, where the client has a client network address and the server has a destination network address. The apparatus includes a port coupled to the server to receive packets addressed to the destination network address. A client validation system coupled to the port,

upon validating the client, allows the client to access the server based upon the client network address.

Embodiments of the invention may include one or more of the following features. When the client validation system allows the client to access the server, the client validation system can configure the port to selectively communicate with the client network address. When the client validation system allows the client to access the server, the client validation system can configure the port to selectively accept packets from the client network address. The port can drop packets from unvalidated network addresses.

In general, in another aspect, the invention features apparatus for establishing an access-controlled communications path across a network between a client coupled to the network and a network resource, where the client has a client network address. The apparatus includes a publicly-accessible port coupled to the network to receive packets addressed to the apparatus. An access-controlled port coupled to the network resource requires validation for access. A firewall coupled to the publicly-accessible port and the access-controlled port blocks packets from unvalidated network addresses. A client validation system coupled to the publicly-accessible port and the firewall, upon validating the client, configures the firewall such that packets from the client are passed through the firewall to the access-controlled port based upon the client network address.

Embodiments of the invention may include one or more of the following features. A timer can be coupled to the client validation system and the firewall, wherein the timer configures the firewall, after the client has been validated, such that after a predetermined time period, packets from the client are no longer passed through the

firewall to the access-controlled port until the client is revalidated.

In general, in another aspect, the invention features a storage device tangibly storing a control program, the control program, when coupled to a control device, operating the control device to establish an access-controlled communications path across a network between a client and a network resource, where the client has a client network address. The control program is configured to operate the control device to perform functions which include validating the client to produce a validated client network address, and allowing access to the network resource based upon the destination network address.

Advantages of the invention may include one or more of the following. Remote or traveling users can access and transmit confidential information via a network such as the Internet without compromising the confidentiality of the information. By accessing a specific HTTP web site and performing a validation routine, the user can achieve an access-controlled communications path from any remote location that can access the Internet. In such a system, "hackers" or other potential intruders will not be able to access the validation system for the access-controlled communications channel. The publicly-accessible portion can be a networked computer with little or no resources to be compromised. By allowing only validated network addresses contact with access-controlled resources, where additional verifications can be made, potential intruders can be better excluded from attempting access to those resources, greatly enhancing security.

These and other features and advantages of the present invention will become more apparent from the following description, drawings, and claims.

DRAWINGS

Figure 1 is block diagram of a data communications network.

Figure 2 is a flow chart of a method for establishing an access-controlled communications path.

Figure 3 is a block diagram of a machine-readable device encoded with software for establishing an access-controlled communications path on a server.

DESCRIPTION

Referring to Figure 1, network 10 is coupled to and allows data communication between first client 20, second client 30, and server 40. First client 20, second client 30, and server 40 all have unique network addresses that correspond to their connection to network 10. First client 20 has a client network address 21 which may be unique and which serves to identify first client 20 to other entities coupled to network 10. Client network address 21 may be an Internet protocol (IP) address. Similarly, server 40, which may be an HTTP server or another network resource, has destination network address 41 which serves to identify, and facilitate data exchange with, server 40. In one embodiment, server 40 supports an HTTP web site which can be accessed via the Internet. Server 40 includes publicly-accessible port 42, access-controlled port 44, client validation system 46, firewall 48, and timer 50.

First client 20 can access the web site supported by server 40 from any remote location that allows access to network 10, e.g., by connecting to an Internet provider via a modem. This initial access is via an unsecured communications path between first client 20 and publicly-accessible port 42.

Once a communications path has been established between first client 20 and publicly-accessible port 42,

client validation system 46 validates first client 20 to determine whether first client 20 should be granted access to access-controlled port 44. Validation may be accomplished through a password system, with an electronic smart card that generates a known sequence of validation codes or sequences, or by using other validation techniques. One particular validation scheme uses a challenge table having a predetermined, enumerated list of validation code sequences. For example, the server may ask the client to enter a validation code sequence corresponding to number 82. The client would then respond by entering the validation code sequence corresponding to entry 82 of the challenge table. These validation code sequences can be intended for a single use only, thus ensuring that no other client can intercept the last-used validation code sequence and use it to gain unauthorized access.

Because validation takes place over an unsecured communications path, the validation system should be devised such that other clients are not able to intercept and then use components of the validation system to gain access to the access-controlled port 44. The use of one-time passwords fulfills this need, because, even if a one-time password is intercepted, it cannot be used again.

Once first client 20 is validated, first client 20 is granted access to an access-controlled network resource such as server 40 via an access-controlled communications path between first client 20 and access-controlled port 44. Client network address 21, corresponding to the now-validated first client 20, is considered a validated network address. Client validation system 46 establishes the access-controlled communications path by instructing firewall 48 to allow

packets from first client 20 to pass through to access-controlled port 44.

During communications over the access-controlled communications path, firewall 48 allows only data packets from validated network addresses to pass through to access- controlled port 44. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server 40 will accept the packets or communicate with the source of incoming communications. Thus, if second client 30, having a different, unvalidated client network address, attempts to send packets to or communicate with access-controlled port 44, firewall 48 will refuse to pass packets to access-controlled port 44. Firewall 48 may drop packets received from second client 30 and from all other unvalidated clients. If firewall 48 drops packets from second client 30, second client 30 will not receive any information as to the disposition of the packets it attempted to send to access-controlled port 44. This is beneficial for security reasons, as it does not provide second client 30 with any information which second client 30 might exploit to gain access to secure information through access-controlled port 44.

After gaining access to access-controlled port 44, first client 20 may perform additional validation steps to gain access to the non-public information available on server 40. The additional validation steps may include another password system. The advantage of having this type of two-tiered validation system is that even if potential intruders discover access-controlled port 44, they will not be allowed to "hack" or experiment with it. Even so, although potential intruders can experiment with publicly-accessible port 42, they will be blocked by firewall 48 and therefore unable to obtain or affect

information that must be accessed through access-controlled port 44.

Once the access-controlled communications path has been established, client validation system 46 can allow the path to be maintained for a predetermined period of time. The time period can be a standard time period, client specific, or set when first client 20 initiates the access-controlled communications path. If the path is to be maintained for a predetermined time period, client validation system 46 can instruct timer 50 to either terminate the access-controlled communications path at the end of the predetermined time period or allow first client 20 to be revalidated and thus maintain the access-controlled communications path.

To keep first client 20 apprised of the status of the access-controlled communications path, timer 50 can provide information to first client 20 about the predetermined time period. This information can also be supplied through client validation system 46. The information provided can include the amount of time remaining in the time period or information on extending the time period. For example, timer 50 may communicate a running clock to first client 20 via a dialog box or other indication of the time remaining before revalidation is required. The client, in turn, can use this information to generate an indicator that displays the information. When the first predetermined time period expires, timer 50 can then prompt first client 20 for an additional validation sequence which, when entered, causes timer 50 to maintain the access-controlled communications path for a second predetermined time period.

In some scenarios, multiple clients may share a single proxy server allowing them to access networks such as the Internet. In such cases, the multiple clients

share the network address of the proxy server. Therefore, both a client and a derivative client may establish access-controlled communications paths with the same destination server 40, wherein each of the two access-controlled communications paths is established for a predetermined time period. Client validation system 46, after opening firewall 48 to packets from the shared network address, can compare the two predetermined time periods and determine which is longer. Based on the comparison, the longer time period will be used to determine when timer 50 closes firewall 48 to packets from the shared network address. This can also apply to any other case where a plurality of clients share the same network address. Because firewall 48 can remain open for the longest time period of any client which has been validated, ignoring the shorter time periods of other clients at the same network address reduces the overhead which must be managed by the system without altering performance.

Referring to Figure 2, an access-controlled communications path is established between client 20 and a network resource (e.g., server 40) by first establishing a communications path, which may be an unsecured path, across network 10 between client 20 and destination network address 41 (step 200).

Client 20 is validated (step 202) to produce a validated client network address. If validation fails, destination network address 41 can be instructed to drop packets received from the unvalidated network address (step 204). Validation can be accomplished through the use of one-time passwords or with other techniques, as above.

Once client 20 has been validated, access is allowed to a network resource based upon the validated client network address 21 (step 206). This can include

configuring the network resource to selectively communicate with validated client network address 21, including selectively accepting packets from validated client network address 21. Once the access-controlled communications path is established, the network resource can also block communication with at least one unvalidated network address (e.g., client network address 31). In other words, when an access-controlled communications path is established, the network resource can choose to only accept packets from the particular IP address which has been validated, thus ensuring that unauthorized clients at other IP addresses are unable to gain access to non-public or confidential information. In some applications, this may include opening firewall 48 to packets from validated client network address 21.

Once established, the access-controlled communications path can be terminated after a first predetermined time period. This can help ensure, among other things, that a remote terminal accidentally left connected will not give an unauthorized client access to non-public information. The time remaining in the first predetermined time period is monitored (step 208), and if it has not yet expired, the access-controlled path is maintained (step 210). During the duration of the first predetermined time period, information can be sent to client 20 to keep client 20 aware of the time limitation. This information can include the time remaining in the period, and can also include information on extending the first predetermined time period. Thus, client 20 can monitor how much time remains before the path will be terminated, and he or she can either finish whatever tasks are being performed or extend the time period before the path is automatically terminated.

When the first predetermined time period expires, the client can be revalidated in order to maintain the

access-controlled communications path (step 212). This may also be accomplished at various points within the first predetermined time period. If revalidation is unsuccessful, such as if client 20 has left the remote terminal, the path is terminated (step 214). If revalidation is successful, the access-controlled communications path can be maintained for a second predetermined time period based on the revalidation (step 216). Revalidation can be accomplished by requesting a second predetermined validation sequence from client 20, wherein the access-controlled communications path would be maintained based on the second predetermined validation sequence. The lengths of the various time periods can be configurable for each individual path, or can be a fixed length of time. For example, a particular client may request additional time and, based on the identity of the particular client, a fixed amount of time may be added, the extension of time may be denied, or the client may be allowed to choose how much additional time is granted up to a predetermined maximum.

Once the access-controlled path is terminated, either at the direction of the client 20 or through the expiration of the connection time period, the network resource stops accepting packets from the previously validated client network address until the client network address is again validated. An unauthorized client thereby will not be able to log on through the same terminal (or other IP address) used by the previous authorized client and gain access to privileged information, despite sending messages through the same IP address.

Referring to Figure 3, software 310 for providing session emulation services can be placed upon any machine-readable device 300, such as a floppy disk, CD-ROM, removable hard drive, or other memory device, and

can then be loaded into server 40. Software 310 can include code which, when loaded into server 40, provides the software for establishing a access-controlled communications path between first client 20 and a network resource (e.g., server 40) across network 10 based on the network address associated with first client 20. Software 310 can also include code which, when loaded into a server 40, provides the application software needed to perform validation of first client 20, control the length of time the access-controlled communications path is maintained, and control the disposition of packets received from unvalidated clients.

Establishing an access-controlled communications path allows traveling or other remote clients to access confidential or privileged information over the Internet without compromising the security of the information. For example, a client may log into any terminal with access to the Internet, go to a particular web site, verify his or her authority to access a privileged portion of the web site, and then access the privileged portion without fear of others obtaining information about, or access to, the privileged area. Such a traveling client can generate a challenge table of one-time passwords before traveling and then use those passwords to access the system while away.

The described methods and apparatus provide a low-cost, efficient means of data communication that eliminates the need for clients to carry laptops with them while traveling merely to perform such tasks as using electronic mail, accessing databases, etc. Assuming such a client can access a terminal connected to the Internet, access-controlled communication with a server or other network resource is possible with minimal complexity and no additional hardware.

Clients (such as employees) can access files stored on computers at work while at home merely by accessing the World Wide Web through any Internet Service Provider (ISP). Assuming the employer's computers are connected to the Internet, this can eliminate the need for the company to provide numerous modems to support dial-up capability.

Other embodiments are within the scope of the claims. For example, multiple clients can communicate with each other in a secure environment from any set of Internet-capable terminals. Each client can establish an access-controlled communications path with a particular server or system and then be linked together behind a firewall. Once access-controlled paths are established, secure transmission of messages and data between clients at remote locations can be facilitated without fear of interception.

What is claimed is:

1. A method for establishing an access-controlled communications path across a network between a client and a network resource, the client having a client network address, comprising:

validating the client to produce a validated client network address; and

allowing the client access to the network resource based upon the validated client network address.

2. The method of claim 1 further comprises establishing a communications path between the client and a destination network address coupled to the network resource.

3. The method of claim 1 wherein the step of allowing the client access to the network resource further comprises configuring the network resource to selectively communicate with the validated client network address.

4. The method of claim 2 wherein the step of allowing the client access to the network resource further comprises configuring the network resource to selectively accept packets from the validated client network address.

5. The method of claim 1, wherein when the client terminates the access-controlled communications path, the network resource no longer accepts packets from the client network address until the client network address is again validated.

6. The method of claim 1, wherein communication with at least one unvalidated network address is blocked by the network resource.

7. The method of claim 1, wherein the network resource drops packets from unvalidated network addresses.

8. The method of claim 1, wherein allowing the client access to the network resource further comprises opening a firewall to packets from the validated client network address.

9. The method of claim 2 wherein the step of establishing the communications path between the client and the destination network address further comprises establishing the communications path between the client and a server through the destination network address.

10. The method of claim 9, wherein the server comprises an HTTP server.

11. The method of claim 1 wherein the client network address comprises an IP address.

12. The method of claim 1 further comprises terminating the access-controlled communications path after a first predetermined time period.

13. The method of claim 12 further comprises indicating to the client information related to the first predetermined time period.

14. The method of claim 13, wherein the client generates an indicator that displays the information related to the first predetermined time period.

15. The method of claim 13 wherein the information related to the first predetermined time period comprises time remaining in the first predetermined time period.

16. The method of claim 13 wherein the information related to the first predetermined time period comprises information on extending the first predetermined time period.

17. The method of claim 1 further comprising the steps of:

maintaining the access-controlled communications path for a first predetermined time period;

after the first predetermined time period, revalidating the client; and

maintaining the access-controlled communications path for a second predetermined time period based on revalidation.

18. The method of claim 1 wherein the step of validating further comprises:

requesting a first predetermined validation sequence from the client; and

validating the client based on a response from the client.

19. The method of claim 18 further comprising the step of requesting a second predetermined validation sequence, wherein the access-controlled communications path is maintained based on the second predetermined validation sequence.

20. The method of claim 1 further comprising:

validating a derivative client, wherein the derivative client shares the client network address with the client, wherein the client establishes a first predetermined time period for the access-controlled communications path and the derivative client establishes a second predetermined time period for the access-controlled communications path;

comparing the first predetermined time period with the second predetermined time period to determine the longer time period; and

maintaining the access-controlled communications path based on the longer time period.

21. Apparatus for establishing an access-controlled communications path across a network between a client coupled to the network and a server coupled to the network, the client having a client network address, and the server having a destination network address, comprising:

a port coupled to the server, the port receiving packets addressed to the destination network address; and

a client validation system coupled to the port, the client validation system, upon validating the client, allowing the client to access the server based upon the client network address.

22. The apparatus of claim 21, wherein when the client validation system allows the client to access the server, the client validation system configures the port to selectively communicate with the client network address.

23. The apparatus of claim 22, wherein when the client validation system allows the client to access the

server, the client validation system configures the port to selectively accept packets from the client network address.

24. The apparatus of claim 21, wherein the port drops packets from unvalidated network addresses.

25. Apparatus for establishing an access-controlled communications path across a network between a client coupled to the network and a network resource, the client having a client network address, comprising:

a publicly-accessible port coupled to the network, the publicly-accessible port receiving packets addressed to the network resource;

an access-controlled port coupled to the network resource, the access-controlled port requiring validation for access;

a firewall coupled to the publicly-accessible port and the access-controlled port, the firewall blocking packets from unvalidated network addresses; and

a client validation system coupled to the publicly-accessible port and the firewall, the client validation system, upon validating the client, configuring the firewall such that packets from the client are passed through the firewall to the access-controlled port based upon the client network address.

26. The apparatus of claim 25 further comprising a timer coupled to the client validation system and the firewall, wherein, after the client has been validated, the timer configures the firewall such that after a predetermined time period, packets from the client are no longer passed through the firewall to the access-controlled port until the client is revalidated.

27. A storage device tangibly storing a control program, the control program, when coupled to a control device, operating the control device to establish an access-controlled communications path across a network between a client and a network resource, the client having a client network address, the control program being configured to operate the control device to perform the functions of:

validating the client to produce a validated client network address; and

allowing the client access to the network resource based upon the destination network address.

28. The storage device of claim 27 wherein the control program is further configured to operate the control device to perform the function of establishing a communications path between the client and a destination network address coupled to the network resource.

29. The storage device of claim 27 wherein allowing the client access to the network resource further comprises configuring the network resource to selectively communicate with the validated client network address.

30. The storage device of claim 29, wherein allowing the client access to the network resource further comprises configuring the network resource to selectively accept packets from the validated client network address.

31. The storage device of claim 27, wherein when the client terminates the access-controlled communications path, the network resource no longer accepts packets from the client network address until the client network address is again validated.

32. The storage device of claim 27, wherein communication with at least one unvalidated network address is blocked by the network resource.

33. The storage device of claim 27, wherein the network resource drops packets from unvalidated network addresses.

34. The storage device of claim 27, wherein allowing the client access to the network resource further comprises opening a firewall to packets from the validated client network address.

35. The storage device of claim 28, wherein establishing the communications path between the client and the destination network address further comprises establishing the communications path between the client and a server through the destination network address.

36. The storage device of claim 35, wherein the server comprises an HTTP server.

37. The storage device of claim 27 wherein the client network address comprises an IP address.

38. The storage device of claim 27, wherein the control program is further configured to operate the control device to perform the function of terminating the access-controlled communications path after a first predetermined time period.

39. The storage device of claim 38, wherein the control program is further configured to operate the control device to perform the function of indicating to

the client information related to the first predetermined time period.

40. The storage device of claim 39, wherein the client generates an indicator that displays the information related to the first predetermined time period.

41. The storage device of claim 39, wherein the information related to the first predetermined time period comprises time remaining in the first predetermined time period.

42. The storage device of claim 39, wherein the information related to the first predetermined time period comprises information on extending the first predetermined time period.

43. The storage device of claim 27, wherein the control program is further configured to operate the control device to perform the functions of:

maintaining the access-controlled communications path for a first predetermined time period;

after the first predetermined time period, revalidating the client; and

maintaining the access-controlled communications path for a second predetermined time period based on revalidation.

44. The storage device of claim 27 wherein validating further comprises:

requesting a first predetermined validation sequence from the client; and

validating the client based on a response from the client.

45. The storage device of claim 27, wherein the control program is further configured to operate the control device to perform the function of requesting a second predetermined validation sequence, wherein the access-controlled communications path is maintained based on the second predetermined validation sequence.

46. The storage device of claim 27, wherein the control program is further configured to operate the control device to perform the functions of:

validating a derivative client, wherein the derivative client shares the client network address with the client, wherein the client establishes a first predetermined time period for the access-controlled communications path and the derivative client establishes a second predetermined time period for the access-controlled communications path;

comparing the first predetermined time period with the second predetermined time period to determine the longer time period; and

maintaining the access-controlled communications path based on the longer time period.

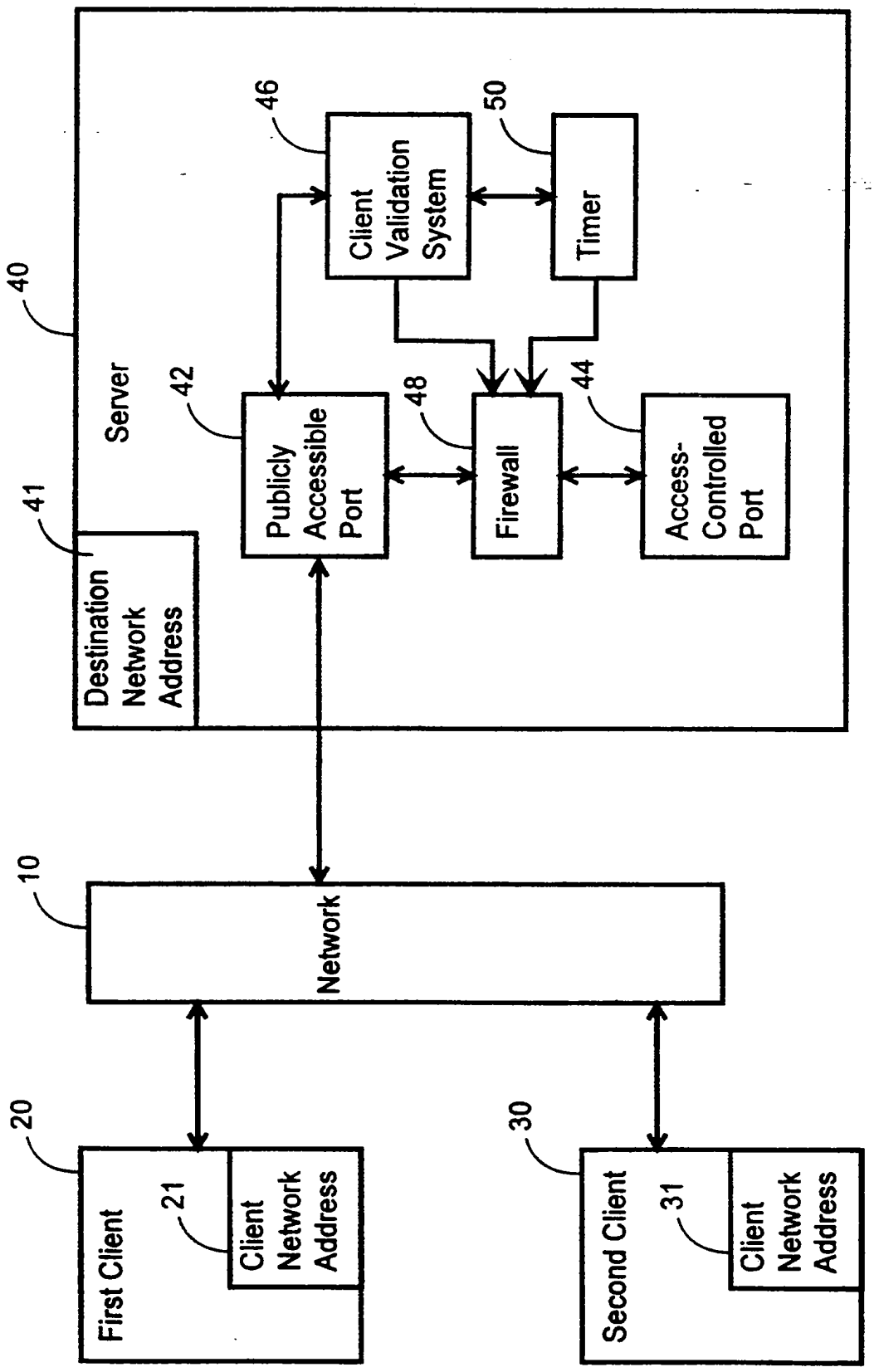
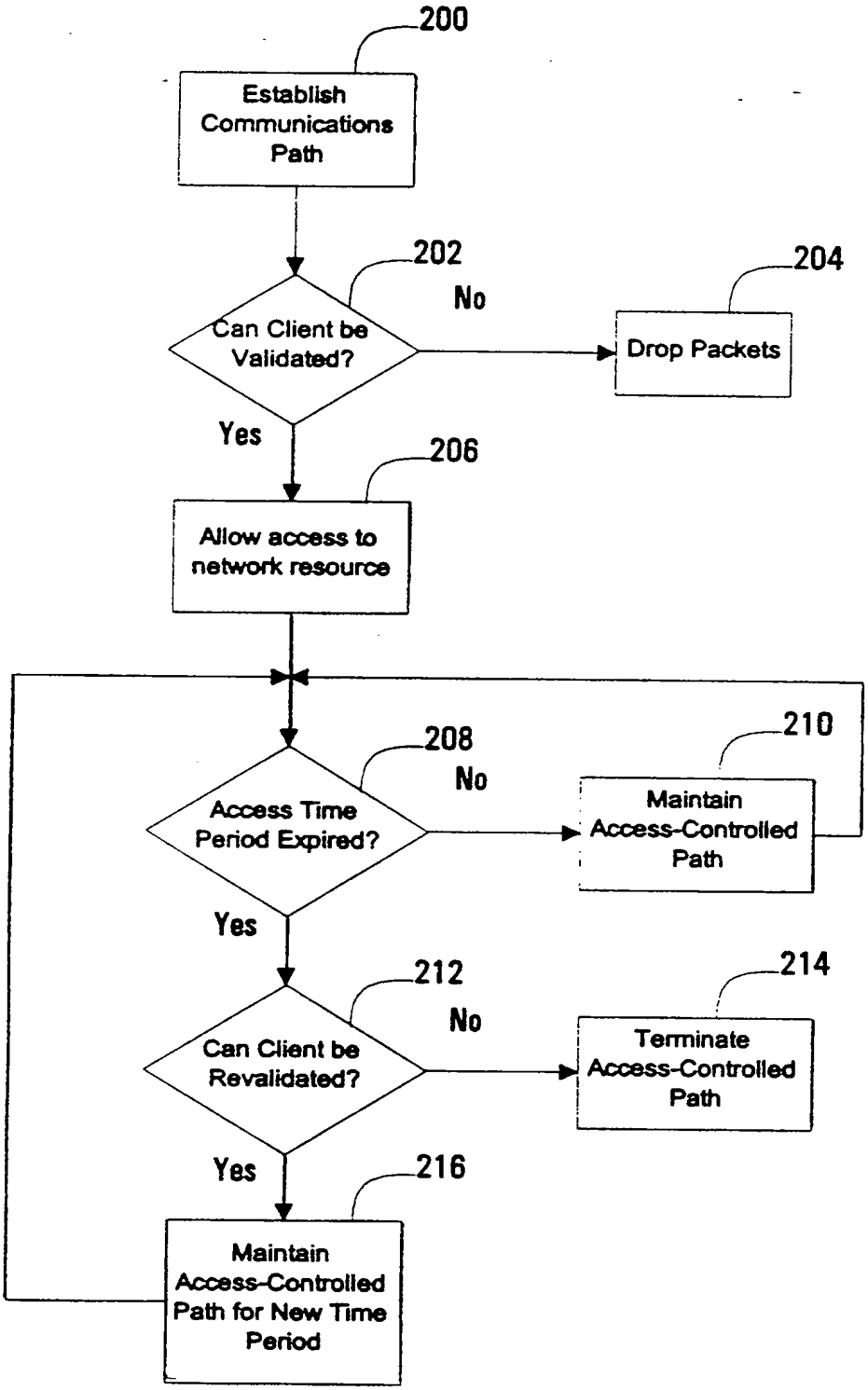

Server
40
Client Validation System
46
Timer
50
Publicly Accessible Port
42
Firewall
48
Access-Controlled Port
44
Destination Network Address
41
Network
10
First Client
20
Client Network Address
21
Second Client
30
Client Network Address
31

Fig. 1

Fig. 2



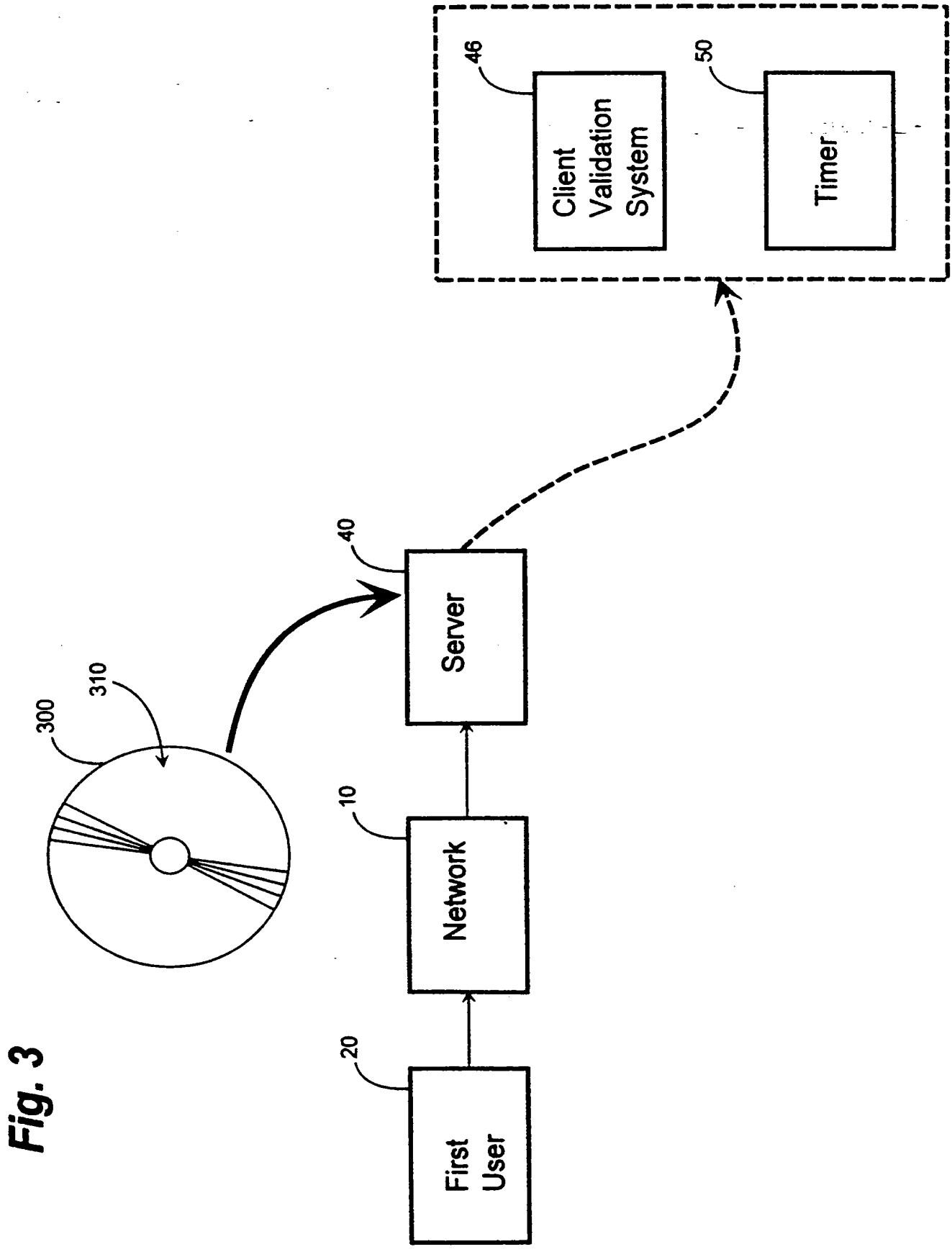

46
Client Validation System
50
Timer
40
Server
310
300
10
Network
20
First User

Fig. 3

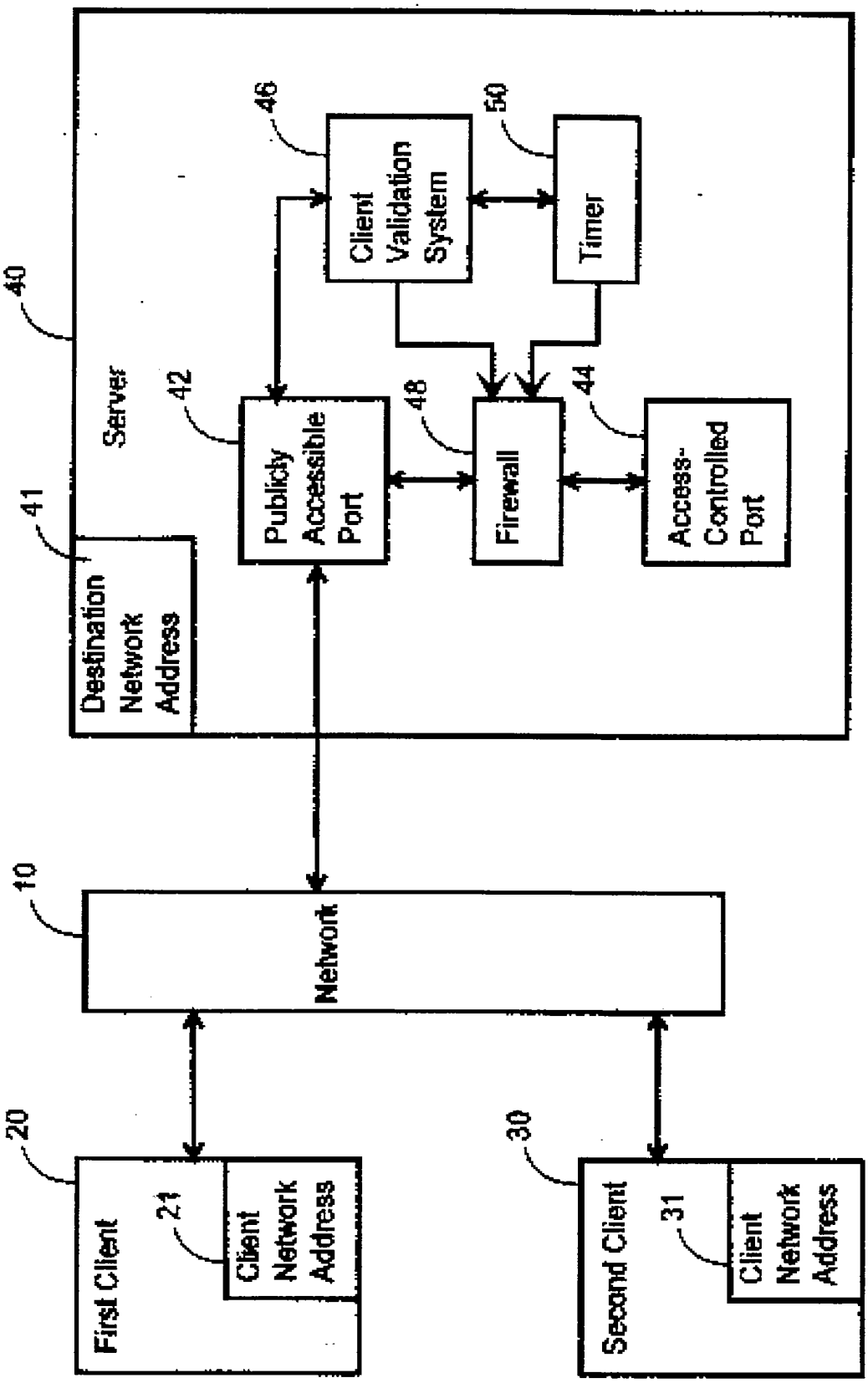
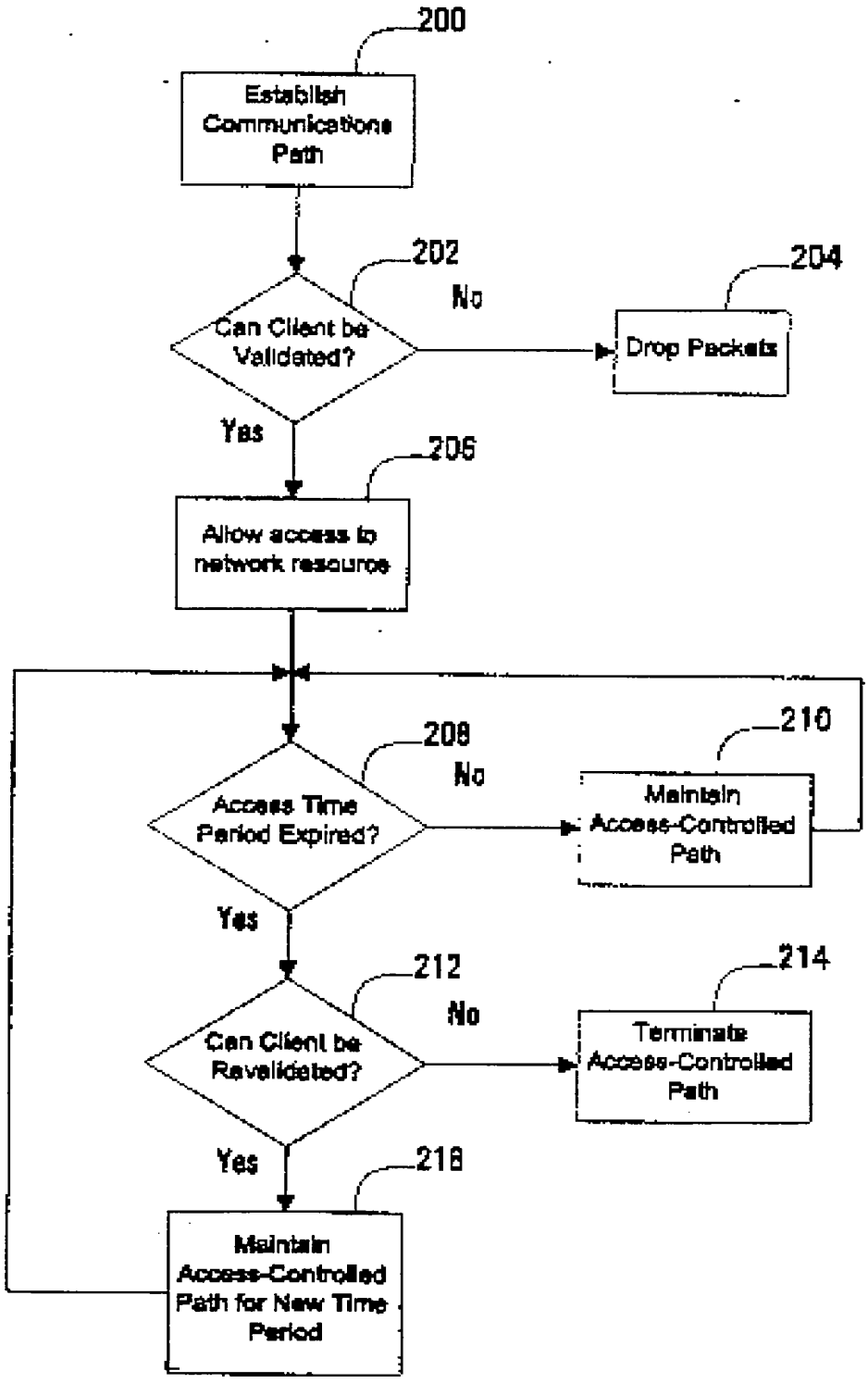


Fig. 1

Fig. 2


200
Establish Communications Path
202
Can Client be Validated?
No
204
Drop Packets
Yes
206
Allow access to network resource
208
Access Time Period Expired?
No
210
Maintain Access-Controlled Path
Yes
212
Can Client be Revalidated?
No
214
Terminate Access-Controlled Path
Yes
216
Maintain Access-Controlled Path for New Time Period

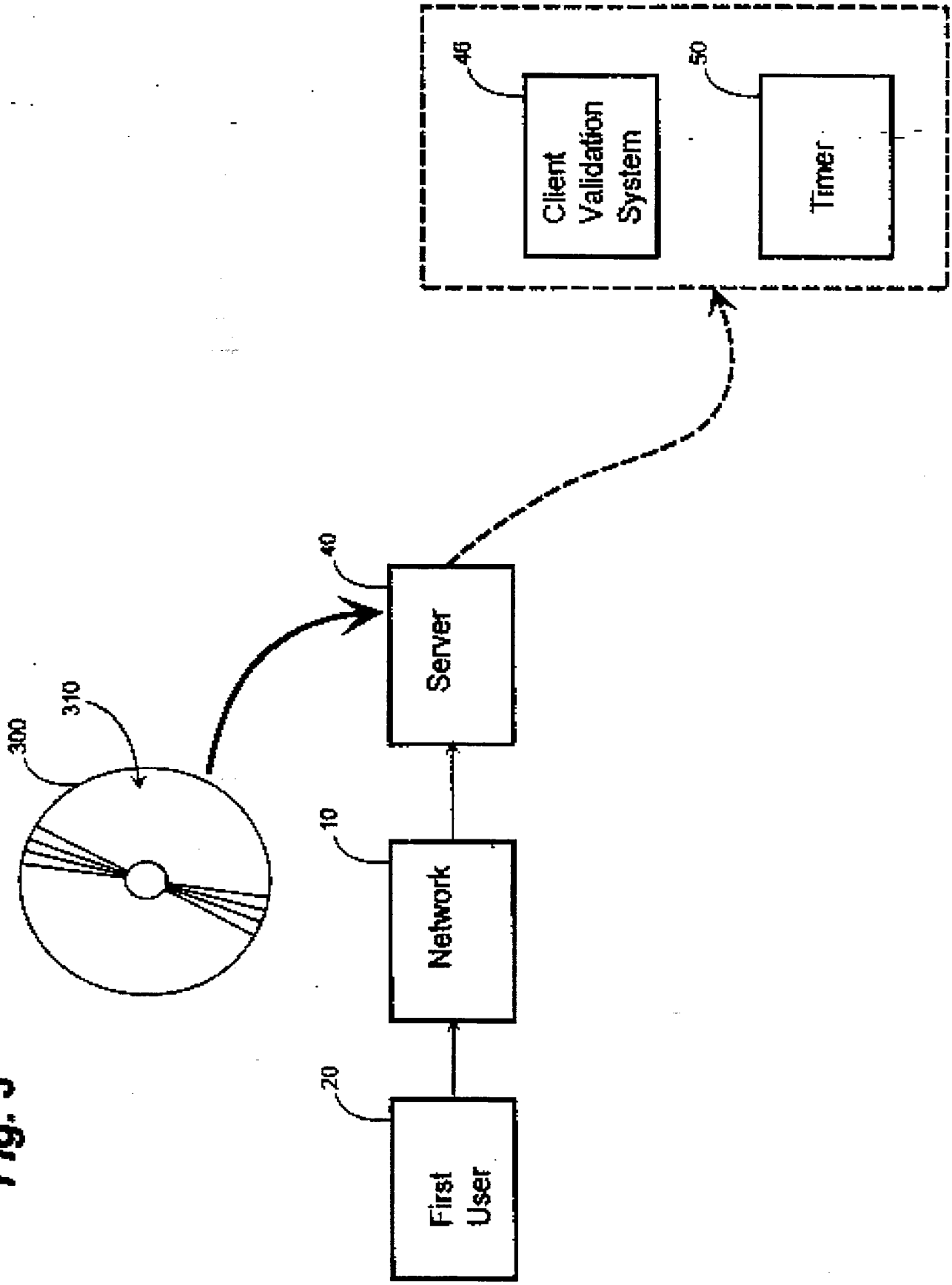


Fig. 3

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **G06F 13/00, H01J 1/00**	**A3**	**(11) International Publication Number:** **WO 99/13448** **(43) International Publication Date:** 18 March 1999 (18.03.99)

(21) International Application Number: PCT/US98/19239

(22) International Filing Date: 11 September 1998 (11.09.98)

(30) Priority Data:
08/928,360 12 September 1997 (12.09.97) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, MS PAL1–521, Palo Alto, CA 94303 (US).

(72) Inventor: KALAJAN, Kevin, E.; 2900 Broadway #F, Redwood City, CA 94062 (US).

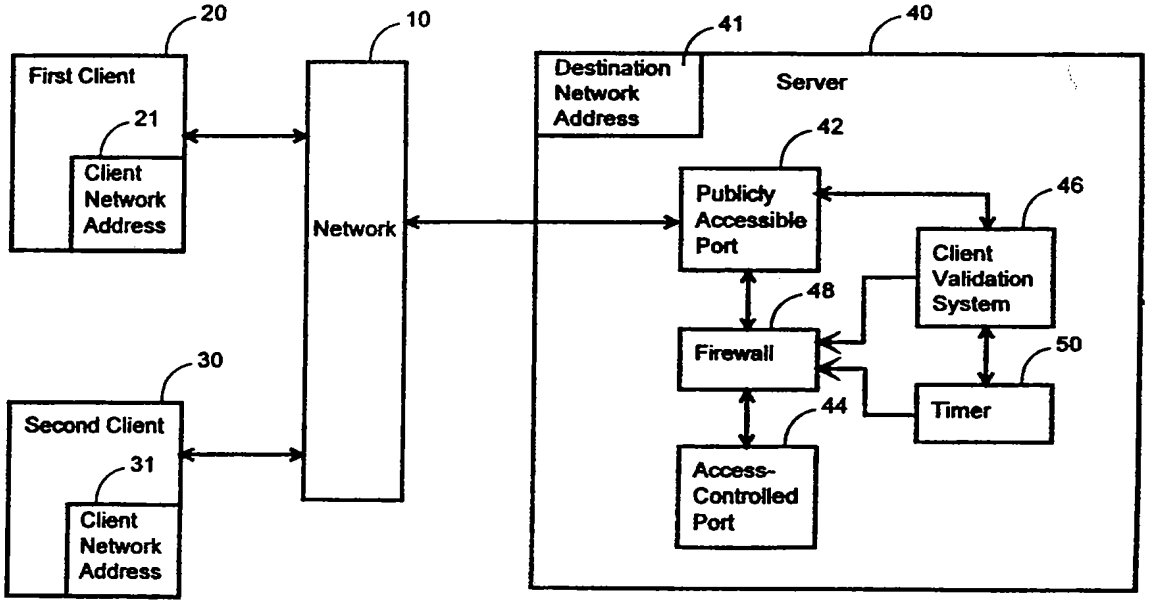
(74) Agent: SOBON, Wayne, P.; Fish & Richardson P.C., Suite 100, 2200 Sand Hill Road, Menlo Park, CA 94025 (US).

(81) Designated States: CA, IL, JP, MX, NO, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(88) Date of publication of the international search report:
6 May 1999 (06.05.99)

(54) Title: REMOTE ACCESS–CONTROLLED COMMUNICATION



(57) Abstract

A method for establishing an access controlled communications path across a network (10) between a client (20, 30) and a network resource (41), the client (20, 30) having a client network address (21, 31), includes validating the client (20, 30) to produce a validated client network address (46), and allowing the client (20, 30) access to the network resource (41) based upon the validated client network address (46).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/19239

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 13/00; H01J 1/00

US CL : 395/187.01, 200.55, 200.59, 200.57

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/187.01, 200.55, 200.59, 200.57

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,E	US 5,812,819 A (RODWIN et al.) 22 September 1998, see entire document.	1-46
Y,P	US 5,778,174 A (CAIN) 07 July 1998, see entire document.	1-46
Y,P	US 5,774,650 A (CHAPMAN et al.) 30 June 1998, see entire document.	1-46
A	US 5,560,008 A (JOHNSON et al.) 24 September 1996, see entire document.	1-4, 21-27
A,E	US 5,815,664 A (ASANO) 29 September 1998, see entire document.	1-4, 21-28
A,E	US 5,828,833 A (BELVILLE et al.) 27 October 1998, see entire document.	1-46

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search

24 NOVEMBER 1998

Date of mailing of the international search report

25 FEB 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

NORMAN WRIGHT Joni Hill

Telephone No. (703) 305-9600

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/19239

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 5,781,550 A (TEMPLIN et al.) 14 July 1998, see entire document.	1-4 and 21-28
Y,P	US 5,805,803 A (BIRRELL et al.) 08 September 1998, see abstract and background.	1-4 and 21-28
A,E	US 5,828,832 A (HOLDEN et al.) 27 October 1998, abstract and background.	1-4, and 21-27
A,E	US 5,822,518 A (OOKI et al.) 13 October 1998, see entire document.	1-4 and 21-28
A,E	US 5,835,726 A (SHWED et al.) 10 November 1998, see entire document.	1-46

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/19239

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS, STN- WPIDS, Inspec, Compuscience, Compendex search terms: client, valida?, authoriz?, authentic?, extend, timer, connect?, period, reauthoriza?, revalida?, access, restart, reset, communication, channel.